ON INVERSE SYSTEMS OF ARTINIAN GORENSTEIN ALGEBRAS

STEFAN O. TOHANEANU

ABSTRACT. Let I be a homogeneous ideal in $R = \mathbb{K}[x_0, \ldots, x_n]$, such that R/I is an Artinian Gorenstein ring. A famous theorem of Macaulay says that in this instance I is the ideal of polynomial differential operators with constant coefficients that cancel the same homogeneous polynomial F. A major question related to this result is to be able to describe F in terms of the ideal I. In this note we give a partial answer to this question, by analyzing the case when I is the Artinian reduction of the ideal of a reduced (arithmetically) Gorenstein zero-dimensional scheme $\Gamma \subset \mathbb{P}^n$. We obtain F from the coordinates of the points of Γ. We also describe how to solve systems of multivariate polynomials having finite dimensional solution, using inverse systems.

1. INTRODUCTION

Let $\mathbb{K}$ be a field of characteristic zero, and let $R = \mathbb{K}[x_0, \ldots, x_n]$ be the ring of homogeneous polynomials with coefficients in $\mathbb{K}$. Let $I \subset R$ be a homogeneous ideal.

The ring R/I is called *Artinian* if R/I is a finite dimensional vector space over $\mathbb{K}$. Equivalently, $\mathrm{ht}(I) = n + 1$ (i.e., the Krull dimension of R/I is zero), or there exists a positive integer $d > 0$ such that $(R/I)_d = 0$ (i.e., every homogeneous polynomial of degree d is an element of I).

An Artinian ring R/I is called *Gorenstein* if $Soc(R/I) := \{a \in R/I \mid \langle x_0, \ldots, x_n \rangle a = 0\}$ (this is called the *socle* of R/I) is a 1-dimensional $\mathbb{K}-$vector space. It is not difficult to see that if $s+1$ is the least integer such that $(R/I)_{s+1} = 0$ and if R/I is Gorenstein, then $Soc(R/I) = (R/I)_s$ and therefore, $\dim(R/I)_s = 1$. In this instance we call s to be the *socle degree* of R/I.

An *arithmetically Gorenstein* scheme means a projective scheme whose coordinate ring localized at any of its prime ideals is a local Gorenstein ring

2010 *Mathematics Subject Classification.* Primary 13N10; Secondary: 13H10, 14C05, 13P15.

Key words and phrases. Artinian Gorenstein ring, Macaulay inverse system, XL algorithm, zero-dimensional scheme.

Author's address: Department of Mathematics, Western University, London, Ontario N6A 5B7, Canada; Phone: 519-661-2111 Ex: 86528; Email: stohanea@uwo.ca.

(i.e., it is a local ring that is Cohen-Macaulay and the canonical module is free of rank 1). In terms of the graded minimal free resolution, if $X \subset \mathbb{P}^n$ is a $d-$dimensional scheme with defining ideal I_X, then X is arithmetically Gorenstein if and only if R/I_X has the graded minimal free resolution as an $R-$module:

$$0 \to F_k \to \cdots \to F_1 \to R \to R/I_X \to 0,$$

where $k = n-d$ and $F_k \simeq R(-\alpha)$. $\alpha - k$ will be called also the *socle degree* of X, for obvious reasons, and coincides with the Castelnuovo-Mumford regularity $reg(R/I_X)$ of X.

A famous theorem of Macaulay ([13]), that is known in the literature as *Macaulay's Inverse System Theorem*, states that the Artinian ring R/I is Gorenstein if and only if I is the ideal of a system of homogeneous polynomial differential operators with constant coefficients having a unique solution. More precisely, let $S = \mathbb{K}[y_0, \ldots, y_n]$ be the homogeneous polynomial ring with coefficients in $\mathbb{K}$ and variables $y_0, \ldots, y_n$. R acts on S by

$$x_0^{i_0} \cdots x_n^{i_n} \circ y_0^{j_0} \cdots y_n^{j_n} = \frac{\partial^{i_0+\cdots+i_n}}{\partial y_0^{i_0} \cdots \partial y_n^{i_n}}(y_0^{j_0} \cdots y_n^{j_n}),$$

extended by linearity. Then R/I is Artinian Gorenstein if and only if $I = Ann(F) := \{f \in R | f \circ F = 0\}$, for some $F \in S$ (we are going to denote the elements in S with capital letters). The best surveys on applications of inverse systems and also, very good introductions to this subject are [8] and [11], and of course, the citations therein.

Immediate consequences of Macaulay's Inverse System Theorem are the following: (1) F has degree equal to the socle degree s of R/I; (2) the Hilbert function of R/I in degree i (i.e., $HF(R/I, i) = \dim_{\mathbb{K}}(R/I)_i$) equals the dimension of the vector space spanned by the partial derivatives of order i of F; (3) from the previous item one can obtain the symmetry of the Hilbert function of R/I, i.e., $HF(R/I, i) = HF(R/I, s-i)$, for all $i = 0, \ldots, s$.

To my knowledge, it is not known how the shape of F makes the distinction between Artinian complete intersections and Artinian Gorenstein rings, as the first class is included in the second. On this idea, a question asked by Tony Geramita is if one can determine F from the the minimal generators of an Artinian complete intersection ideal I, at the same time making this distinction. Our notes follow the same type of direction: we determine F for the case when I is the Artinian reduction[1] of the ideal of a zero-dimensional reduced Gorenstein scheme (i.e., a Gorenstein set of points). F is determined uniquely from the homogeneous coordinates of

[1]By Artinian reduction we understand Artinian reduction by linear forms.

the points that form this scheme: $F = \sum c_i L_i^r$, where L_i is the dual form of each point P_i in this set, r is the regularity, and c_i are nonzero constants, the sum being taken over all points in the set. This result resembles to [2, Theorem 3.8], the difference being that for a Gorenstein set of points, we specify who are the constants c_i in the decomposition $F = \sum c_i L_i^r$, and our approach avoids using the computational arguments presented in [2] (e.g., linear algebra associated to Hankel operators).

At the same time, similar ideas can be found in the work of Cho and Iarrobino ([3]), especially Proposition 1.13, and more generally to Theorem 3.3. There, the situation is more general than ours: let I be the defining ideal of a zero-dimensional scheme in $\mathbb{P}^n$ (saturated in the case of Proposition 1.13, respectively locally Gorenstein in the case of Theorem 3.3). The goal of these results is to determine *the inverse system* of I, which is by definition: $I^{-1} := \oplus_j (I^{-1})_j$, where $(I^{-1})_j := \{G \in S_j | f \circ G = 0, \text{ for any } f \in I_j\}$. Also these results present conditions for the inverse system I^{-1} to determine I uniquely. One needs to mention that the starting point of the above mentioned results is the celebrated theorem of Emsalem and Iarrobino ([7, Theorems IIA and IIB]). Let us remain in the situation of reduced zero-dimensional schemes ([7, Theorem I]). Suppose $Z = \{P_1, \ldots, P_m\} \subset \mathbb{P}^n$, and let $L_i \in S$ be the associated (dual) linear form of P_i. Then $(I_Z^{-1})_j = \text{Span}_{\mathbb{K}}\langle L_1^j, \ldots, L_m^j \rangle$, and $HF(R/I_Z, j) = \dim_{\mathbb{K}}(I_Z^{-1})_j$.

As one can see from our result, if one takes the Artinian reductions of these schemes, the inverse system becomes very concrete and easy to determine (at least with the Gorenstein assumption), as long as one knows $V(I)$. Also we are going to investigate when is $Ann(F)$ the Artinian reduction of a reduced zero-dimensional Gorenstein scheme. In the second part we put together the papers of [5] and [17] to describe a method for solving systems of multivariate polynomials that have a zero-dimensional saturated solution, using inverse systems.

Inverse systems occur naturally in the theory of systems of PDE's with constant coefficients, and similar results to the ones described above appear in the literature from this direction of study.[2] In 1986, a theorem of Stiller ([20, Theorem 1.1]) determines the dimension of I^{-1}, thought also as the solution of such systems of PDE's, in the genereic case and when R/I is Artinian. Also, inverse systems are put to great use in the theory of splines approximation (e.g., [9]), and also in the study of Weak Lefschetz Property

[2]and sometimes, without the knowledge of one another (e.g., [18, Theorem 4.1], published one year later, is an immediate application of Emsalem-Iarrobino theorem).

of Artinian algebras (e.g., [14], [10]). Concerning the later, it would be interesting to see if our main result can bring some insights towards answering [16, Question 3.8].

2. Inverse systems of Artinian reductions of reduced zero-dimensional Gorenstein schemes

First we present a preparatory lemma. In a general form, this lemma can be found as [12, Lemma 1.1]. For an Artinian ring R/I as seen in the introduction, denote $s(R/I)$ the minimum positive integer d such that $(R/I)_{d+1} = 0$ and $(R/I)_d \neq 0$. In case R/I is Gorenstein, $s(R/I)$ is the socle degree of R/I.

Lemma 2.1. *Let I and J be two ideal in R, such that $I \subseteq J$, and R/I and R/J are both Artinian Gorenstein rings. If $s(R/I) = s(R/J)$, then $I = J$.*

Proof. The proof follows immediately from the cited Socle Lemma of Kustin and Ulrich. Just observe that in the case of Gorenstein Artinian rings, $Soc(R/I)$ and $Soc(R/J)$ are one-dimensional graded vector spaces generated in degrees $s(R/I)$ and $s(R/J)$, respectively. And these degrees are equal from hypotheses.

Another simple proof comes from the following linear algebra argument. Suppose $I = Ann(F)$ and $J = Ann(G)$, with $F, G \in S$. Denote $s = s(R/I) = \deg(F) = s(R/J) = \deg(G)$, and suppose

$$F = \sum_{i_0+\cdots+i_n=s} c_{i_0,\ldots,i_n} y_0^{i_0} \cdots y_n^{i_n} \text{ and } G = \sum_{j_0+\cdots+j_n=s} d_{j_0,\ldots,j_n} y_0^{j_0} \cdots y_n^{j_n}.$$

If $f \in I_s \subseteq J_s$, then the coefficients of f form a solution of the homogeneous system of two equations in variables indexed by the monomials of degree s in R:

$$\begin{aligned} \cdots + i_1! \cdots i_n! c_{i_0,\ldots,i_n} Z_{i_0,\ldots,i_n} + \cdots &= 0 \\ \cdots + i_1! \cdots i_n! d_{i_0,\ldots,i_n} Z_{i_0,\ldots,i_n} + \cdots &= 0. \end{aligned}$$

The dimension of the solutions space is the number of variables (i.e. $\dim R_s$) minus the rank of the matrix of the system. Since all elements of I_s are solutions, the dimension of the solutions space is $\geq \dim R_s - 1$. So the rank of the matrix of the system is 1, which leads to F and G being a nonzero scalar multiple of each other. □

Let $Z = \{P_1, \ldots, P_m\} \subset \mathbb{P}^n$ be a reduced zero-dimensional Gorenstein scheme. Let $I_Z \subset R := \mathbb{K}[x_0, \ldots, x_n]$ be the ideal of Z, and assume $reg(R/I_Z) = r$ (which is the same as the socle degree of R/I_Z).

Suppose that $P_i = [a_{i,0}, a_{i,1}, \ldots, a_{i,n}]$, for $i = 1, \ldots, m$, and let $\ell \in R$ be a linear form such that $\ell(P_i) \neq 0$ for all $i = 1, \ldots, m$ (i.e., ℓ is a non-zero divisor in R/I_Z). In these conditions we know that

$$\langle I_Z, \ell \rangle = Ann(F),$$

for some $F \in S := \mathbb{K}[y_0, \ldots, y_n]$ of degree r.

The goal is to find F from the coordinates of the points P_i. For each P_i consider the associated linear form

$$L_i = a_{i,0}y_0 + a_{i,1}y_1 + \cdots + a_{i,n}y_n.$$

Then we have:

Theorem 2.2. *There exist the nonzero constants $c_1, \ldots, c_m \in \mathbb{K}$, unique up to multiplication by a nonzero scalar, such that*

$$\langle I_Z, \ell \rangle = Ann(F),$$

where $F = c_1L_1^r + \cdots + c_mL_m^r$.

The c_i's are the unique nonzero constants such that

$$c_1\ell(P_1)L_1^{r-1} + \cdots + c_m\ell(P_m)L_m^{r-1} = 0.$$

Proof. It is enough to show $\langle I_Z, \ell \rangle \subseteq Ann(F)$. If we know this inclusion, then the equality follows immediately from Lemma 2.1.

Let $f \in I_Z$ of degree d. Then $f \circ L_j^r = 0$ for all $j = 1, \ldots, m$. This follows immediately if $d \geq r + 1$. Otherwise, suppose $d \leq r$, and suppose $f = \sum_{i_0+\cdots+i_n=d} \alpha_{i_0,\ldots,i_n} x_0^{i_0} \cdots x_n^{i_n}$.

Observe that $x_0^{i_0} \cdots x_n^{i_n} \circ L_j^r = x_1^{i_1} \cdots x_n^{i_n} \circ (r - i_0)! a_{j,0}^{i_0} L_j^{r-i_0} = \cdots = (r-d)! a_{j,0}^{i_0} \cdots a_{j,n}^{i_n} L_j^{r-d}$. So

$$f \circ L_j^r = (r-d)! f(P_j) L_j^{r-d} = 0.$$

We obtain

$$I_Z \subset Ann(c_1L_1^r + \cdots + c_mL_1^r), \text{ for any constants } c_i \in \mathbb{K}.$$

To mention here that this argument is at the base of all the important results in the theory of inverse systems, as can be observed, for example, in [8] and [11].

Now we need to show that there exist the nonzero constants $c_1, \ldots, c_m \in \mathbb{K}$, unique up to multiplication by scalars, such that

$$\ell \circ (c_1L_1^r + \cdots + c_mL_m^r) = 0.$$

Equivalently, we have to find the unique, nonzero d_i such that

$$\underbrace{c_1\ell(P_1)}_{d_1} L_1^{r-1} + \cdots + \underbrace{c_m\ell(P_m)}_{d_m} L_m^{r-1} = 0.$$

We have that for any i

$$L_i^{r-1} = \sum_{j_0+\cdots+j_n=r-1} A_{j_0,\ldots,j_n} a_{i,0}^{j_0} a_{i,1}^{j_1} \cdots a_{i,n}^{j_n} y_0^{j_0} y_1^{j_1} \cdots y_n^{j_n},$$

where $A_{j_0,\ldots,j_n}$ are "multinomial" coefficients that do not depend on i.

Grouping the terms of the sum $d_1 L_1^{r-1} + \cdots + d_m L_m^{r-1}$ by the monomials $y_0^{j_0} y_1^{j_1} \cdots y_n^{j_n}$, the fact that this sum vanishes is equivalent to:

$$\text{for any } j_0 + \cdots + j_n = r-1 \text{ we have } \sum_{i=1}^{m} d_i a_{i,0}^{j_0} a_{i,1}^{j_1} \cdots a_{i,n}^{j_n} = 0.$$

This means that

$$(d_1, \ldots, d_m)\mathcal{M}_\phi^\tau = 0,$$

where $\mathcal{M}_\phi^\tau$ is the transposed matrix of the $\binom{r-1+n}{n} \times m$ matrix $\mathcal{M}_\phi$ of the evaluation map

$$\phi : R_{r-1} \longrightarrow \mathbb{K}^m.$$

The map ϕ is built by evaluating the homogeneous polynomials of degree $r-1$ at the points of Z:

$$\phi(x_0^{j_0} x_1^{j_1} \cdots x_n^{j_n}) = (a_{1,0}^{j_0} \cdots a_{1,n}^{j_n}, a_{2,0}^{j_0} \cdots a_{2,n}^{j_n}, \ldots, a_{m,0}^{j_0} \cdots a_{m,n}^{j_n}).$$

We have $reg(I_Z) = reg(R/I_Z) + 1 = r + 1$. By [19, Theorem 7.1.8], the cokernel of ϕ, often denoted $H^1(I_Z(r-1))$, does not vanish. So the map ϕ is not surjective, and hence $\mathrm{rk}\mathcal{M} \leq m-1$. But this translates into the existence of $d_1, \ldots, d_m$ not all zero.

The uniqueness modulo multiplication by the same nonzero scalar comes from the fact that $HF(R/\langle I_Z, \ell\rangle, r) = 1$ and $HF(R/I_Z, r) = m$, and therefore $HF(R/I_Z, r-1) = m-1$. But this means that $\mathrm{rk}\mathcal{M} = m-1$, and hence the dimension of the vectors $(d_1, \ldots, d_m) \in \mathbb{K}^m$ with $(d_1, \ldots, d_m)\mathcal{M}_\phi^\tau = 0$ is exactly one.

To conclude the proof, we need to show that all d_i are nonzero. Consequently, to show that all $c_i \neq 0$. After reordering of the points in Z, let us assume that $c_1 = \cdots = c_k = 0$ and $c_j \neq 0, j \geq k+1$. Let

$$Z' = \{P_{k+1}, \ldots, P_m\} \subsetneq Z.$$

Then $I_Z \subsetneq I_{Z'}$.

Of course we have $I_{Z'} \subset Ann(c_{k+1} L_{k+1}^r + \cdots + c_m L_m^r) = \langle I_Z, \ell\rangle$, and therefore

$$\langle I_Z, \ell\rangle = \langle I_{Z'}, \ell\rangle,$$

where ℓ is a nonzero divisor in $R/I_{Z'}$, since it is a nonzero divisor in R/I_Z. Therefore we get

$$HF(R/I_Z, i) - HF(R/I_Z, i-1) = HF(R/I_{Z'}, i) - HF(R/I_{Z'}, i-1),$$

for all i, leading to $HF(I_{Z'}/I_Z, i) = HF(I_{Z'}/I_Z, i-1)$, for all i, and hence the contradiction $I_Z = I'_Z$. □

In the spirit of [3, Theorem 3.3], a converse to Theorem 2.2 could be phrased into the following question:

Question 2.3. *Let $F = c_1L_1^r + \cdots + c_mL_m^r \in S, c_i \neq 0$ (and by this we also assume that $L_1^r, \ldots, L_m^r$ are linearly independent forms in S_r) and let $Z \subset \mathbb{P}^n$ be the non-degenerate (i.e. not contained in a hyperplane) reduced finite set of points dual to the linear forms L_i. In what conditions is Z arithmetically Gorenstein of regularity r and $Ann(F)$ is an Artinian reduction of I_Z?*

In our situation, when $I = Ann(F)$, and $\deg F = r$, we have $(I^{-1})_j$ to be the $\mathbb{K}-$vector space spanned by the partial derivatives of order $r-j$ of F. Denote this space with $\mathrm{D}^{r-j}(F)$. By the shape of F, it is obvious that $\mathrm{D}^{r-j}(F)$ is a subspace of $\mathrm{Span}_{\mathbb{K}}\langle L_1^j, \ldots, L_m^j\rangle$.

If we want $I = \langle I_Z, \ell\rangle$, with ℓ a linear form which is a nonzero divisor in R/I_Z, from Emsalem-Iarrobino theorem we have

$$\dim \mathrm{D}^{r-j}(F) = \dim \mathrm{Span}_{\mathbb{K}}\langle L_1^j, \ldots, L_m^j\rangle - \dim \mathrm{Span}_{\mathbb{K}}\langle L_1^{j-1}, \ldots, L_m^{j-1}\rangle.$$

• If one requires that $\dim \mathrm{Span}_{\mathbb{K}}\langle L_1^{r-1}, \ldots, L_m^{r-1}\rangle = m-1$, then the regularity of Z is r, and therefore the $h-$vector of R/I_Z equals the Hilbert function of $Ann(F)$, and hence it is symmetric.

• In addition, if we require that for any $1 \leq i_1 < \cdots < i_{m-1} \leq m$, $L_{i_1}^{r-1}, \ldots, L_{i_{m-1}}^{r-1}$ are linearly independent (so Z is Cayley-Bacharach), then from [6, Theorem 5] one has that Z is arithmetically Gorenstein (see also [15, Theorem 1]). The result of Davis, Geramita and Orecchia is an "if and only if" statement, meaning that if Z is reduced zero-dimensional arithmetically Gorenstein then the $h-$vector of I_Z is symmetric and Z is Cayley-Bacharach. Therefore, in the statement of our Theorem 2.2 one can add at the conclusions the properties of $L_1^{r-1}, \ldots, L_m^{r-1}$ observed in this bullet and the previous one.

• From the previous two bullets, one obtains that there exist unique (up to multiplication) nonzero constants $d_1, \ldots, d_m$ such that $d_1L_1^{r-1} + \cdots + d_mL_m^{r-1} = 0$. The existence of $\ell \in R_1$ such that $Ann(F) = \langle I_Z, \ell\rangle$ is equivalent to finding the linear form ℓ such that $\ell(P_i) = \frac{d_i}{c_i}$ for all $i = 1, \ldots, m$. If $P_i = [a_{i,0}, \ldots, a_{i,n}], i = 1, \ldots, m$, this interpolation problem

is equivalent to the $m \times (n+2)$ matrix

$$\begin{pmatrix} a_{1,0} & \cdots & a_{1,n} & -d_1/c_1 \\ a_{2,0} & \cdots & a_{2,n} & -d_2/c_2 \\ \vdots & & \vdots & \vdots \\ a_{m,0} & \cdots & a_{m,n} & -d_m/c_m \end{pmatrix}$$

having rank $n+1$.

Example 2.4. Consider $F = y_2^2 + (y_0+y_1+y_2)^2 - (y_0+y_2)^2 - (y_1+y_2)^2$. Then

$$Z = \{[0,0,1],[1,1,1],[1,0,1],[0,1,1]\} \subset \mathbb{P}^2.$$

Observe that

$$\underbrace{y_2}_{L_1} + \underbrace{(y_0+y_1+y_2)}_{L_2} - \underbrace{(y_0+y_2)}_{L_3} - \underbrace{(y_1+y_2)}_{L_4} = 0$$

and that any three of the linear forms L_1, L_2, L_3, L_4 are linearly independent.

The rank of $\begin{pmatrix} 0 & 0 & 1 & -1 \\ 1 & 1 & 1 & -1 \\ 1 & 0 & 1 & -1 \\ 0 & 1 & 1 & -1 \end{pmatrix}$ is precisely 3. The kernel of the matrix consists of vectors $\begin{pmatrix} 0 & 0 & a & a \end{pmatrix}$, giving $\ell = x_2$.

So $\langle I_Z, x_2 \rangle = Ann(F) = \langle x_0^2, x_1^2, x_2 \rangle$, which checks with the fact that $I_Z = \langle x_0(x_0-x_2), x_1(x_1-x_2) \rangle$.

The decomposition of $F = 2y_0y_1$ as a sum of powers of linear forms is not unique: $F = (y_0+y_1)^2 - y_0^2 - y_1^2$. This type of decompositions are referred to as "The Waring's Problem", and though we will not discuss here about this famous problem, we need to mention the full surveys on the subject covered in [8] and [11]. Also, a very recent progress on these decompositions was made by J. Brachat ([1, Section 4]). Related to our Question 2.3 is [2, Theorem 3.8] (or [1, Théorème 4.4.11]) which says that a form of degree r is a sum of powers of s linear forms if and only if a certain Hankel operator has rank s and its kernel thought as an ideal in R is a radical ideal. The general idea on who is this operator can be viewed in Section 3.1 below: knowing the coefficients of F (i.e., $\beta! b_\beta$), one wants to find the coefficients of f (i.e., a_α) using $\mathcal{A}_f \cdot \overline{b} = 0$. This equation can be arranged such that the coefficients of f are in the kernel of a quasi-Hankel matrix with entries the coefficients of F.

Going back to our example, we cannot pick Z to be the set $\{[1,1,0],[1,0,0],[0,1,0]\} \subset \mathbb{P}^2$, because these three points are on the projective line $x_2 = 0$, and therefore Z would be degenerate.

3. SOLVING SYSTEMS OF MULTIVARIATE HOMOGENEOUS POLYNOMIALS THROUGH INVERSE SYSTEMS

Let $I = \langle f_1, \ldots, f_m \rangle \subset R = \mathbb{K}[x_0, \ldots, x_n]$ be a saturated homogeneous ideal of codimension (i.e., height) equal to n. Let $(I^{-1})_d \subset S_d$, where $S = \mathbb{K}[y_0, \ldots, y_n]$, be the inverse system of degree d of I.

Let $X = Z(I) \subset \mathbb{P}^n$ be the solution of the system of equations

$$f_1 = \cdots = f_m = 0,$$

in other words X is the (arithmetically Cohen-Macaulay) zero-dimensional scheme with defining ideal I. The goal of this section is to find X from the inverse system of I.

To mention here that [3, Theorem 3.3], and the relevant Examples 3.8 and 3.9 after this result, determine the generators of I if one has knowledge **only** about I^{-1}. "Unfortunately" I is already given to us in terms of its generators.

3.1. **Finding the inverse system from generators.** Proposition 1.13 in [3] gives a qualitative answer to the title of this subsection. Since we are interested in quantitative resolution to this problem, we turn to a more computational approach, following Sections 3.5 and 4.2 in [17].

In what follows $\alpha = (\alpha_0, \ldots, \alpha_n)$ is a multi-index. These indices are partially ordered by $\alpha \leq \beta$ iff $\alpha_i \leq \beta_i, i = 0, \ldots, n$. Let $\alpha! = \prod_{i=0}^n \alpha_i!$ and $|\alpha| = \sum_{i=0}^n \alpha_i$.

Let $x^\alpha := x_0^{\alpha_0} \cdots x_n^{\alpha_n} \in R$ and $y^\beta := y_0^{\beta_0} \cdots y_n^{\beta_n} \in S$. By an easy computation (see also [8, Proposition 2.1]) we have

$$x^\alpha \circ y^\beta = \begin{cases} 0, \alpha \not\leq \beta; \\ \frac{\beta!}{(\beta-\alpha)!} y^{\beta-\alpha}, \alpha \leq \beta. \end{cases}$$

Let $f = \sum_{|\alpha|=p} a_\alpha x^\alpha \in R$ be homogeneous of degree p. The goal is to find $F = \sum_{|\beta|=q} b_\beta y^\beta \in S$ homogeneous of degree $q \geq p$ such that $f \circ F = 0$. If $q < p$ the vanishing is trivial.

From the linearity of differential operators and with the calculations we did above for monomials, we can write

$$\begin{aligned} f \circ F &= \sum_{|\alpha|=p} \Big(\sum_{\beta \geq \alpha, |\beta|=q} \frac{\beta!}{(\beta-\alpha)!} a_\alpha b_\beta y^{\beta-\alpha} \Big) \\ &= \sum_{|\alpha|=p} \Big(\sum_{|\gamma|=q-p} \frac{(\alpha+\gamma)!}{\gamma!} a_\alpha b_{\alpha+\gamma} y^\gamma \Big) \\ &= 0. \end{aligned}$$

So, for every $|\gamma| = q - p$ we need to have

$$\sum_{|\alpha|=p} a_\alpha (\alpha+\gamma)! b_{\alpha+\gamma} = 0.$$

The matrix representation of this homogeneous system of equations can be written as follows:

$$\mathcal{A}_f \cdot \bar{b} = 0,$$

where $\bar{b} = \begin{pmatrix} q!b_{(q,0,\ldots,0)} \\ \vdots \\ \beta! b_\beta \\ \vdots \\ q! b_{(0,0,\ldots,q)} \end{pmatrix}$ and $\mathcal{A}_f$ is the matrix with the following characteristics:

- It has $\binom{q-p+n}{n}$ rows, which is the number of indices γ with $|\gamma| = q-p$. The rows are ordered the graded lex ordering on the γ's (e.g., the first row corresponds to $\gamma = (q-p, 0, \ldots, 0)$).
- It has $\binom{q+n}{n}$ columns, which is the number of indices β with $|\beta| = q$. The columns are ordered by the graded lex ordering of the β's (e.g., the first column corresponds to $\beta = (q, 0, \ldots, 0)$).
- The entries of $\mathcal{A}_f$ are

$$(\mathcal{A}_f)_{(\gamma,\beta)} = \begin{cases} 0, \gamma \not\leq \beta; \\ a_{\beta-\gamma}, \gamma \leq \beta. \end{cases}$$

The matrix $\mathcal{A}_f$ is a *quasi-Toeplitz matrix* (as defined in [17, Definition 3.5.1]), and what we did above is to recover, with the same proof, [17, Proposition 3.5.3].

Example 3.1. Suppose $n = 1, p = 2, q = 3$. The γ's are just $(1,0)$ and $(0,1)$. We just have to solve:

$$\begin{pmatrix} a_{(2,0)} & a_{(1,1)} & a_{(0,2)} & 0 \\ 0 & a_{(2,0)} & a_{(1,1)} & a_{(0,2)} \end{pmatrix} \begin{pmatrix} 3!b_{(3,0)} \\ 2!1!b_{(2,1)} \\ 1!2!b_{(1,2)} \\ 3!b_{(0,3)} \end{pmatrix} = 0.$$

The problem of finding the inverse system of degree q, $(I^{-1})_q$, of an ideal $I = \langle f_1, \ldots, f_m \rangle$ reduces to find the solutions of the system

$$\mathcal{A}_{q,I} \cdot \bar{b} = 0,$$

where $\mathcal{A}_{q,I}$ is built by the blocks $\mathcal{A}_{f_i}$:

$$\mathcal{A}_{q,I} = \left(\begin{array}{c} \mathcal{A}_{f_1} \\ \hline \mathcal{A}_{f_2} \\ \hline \vdots \\ \hline \mathcal{A}_{f_m} \end{array} \right).$$

We will call $\mathcal{A}_{q,I}$ to be *the q-inverse system matrix of the ideal I*. This matrix is in fact the generalized Sylvester matrix considered in [17, Section 4.2.2].

When I is Artinian Gorenstein of socle degree q, the above system has a one-parameter solution which gives the coefficients of F in $I = Ann(F)$.

Example 3.2. Find F such that $I = \langle x_1^2 + 2x_0^2, x_0^3 - x_0x_1^2 \rangle = Ann(F)$. Since I is an Artinian complete intersection of a quadric and a cubic, then $\deg(F) = (2-1) + (3-1) = 3$. Solving

$$\begin{pmatrix} 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \\ 1 & 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} 6b_{(3,0)} \\ 2b_{(2,1)} \\ 2b_{(1,2)} \\ 6b_{(0,3)} \end{pmatrix} = 0$$

gives $F = 3y_0^2y_1 - 2y_1^3$.

3.2. **The XL-Algorithm.** Suppose $\mathbb{K}$ is a finite field and suppose we are given $g_i \in \mathbb{K}[x_0, \ldots, x_{n-1}], i = 1, \ldots m$ polynomials, not necessarily homogeneous. Let's assume further that the common zero locus is zero-dimensional. The key problem in cryptography is to find fast ways to solve the system

$$\begin{cases} g_1(x_0, \ldots, x_{n-1}) &= 0 \\ & \vdots \\ g_m(x_0, \ldots, x_{n-1}) &= 0 \end{cases}$$

A very nice algorithm to solve such a system is the XL-Algorithm (see [4], and for connections with Commutative Algebra, see [5]).

The general idea is the following. Suppose $\deg(g_i) = d_i, i = 1, \ldots, m$. Multiply the first equation by all the monomials in x_j's of degree $\leq D - d_1$, the second equation by all the monomials in x_j's of degree $\leq D - d_2$, and so forth multiply the last equation by all monomials of degree $\leq D - d_m$.

We obtain $\sum_{i=1}^{m} \binom{D-d_i+n}{n}$ equations in $\binom{D+n}{n}$ variables, where we think of all the monomials in x_j's of degree $\leq D$ as independent variables.

Suppose we would like to find the value of the n^{th} coordinate of the solution (i.e. x_{n-1}). Order these new variables such that those corresponding to $x_{n-1}^D, \ldots, x_{n-1}, 1$ are the last. Using Gaussian elimination on the matrix

of this new system will result into finding the roots of a univariate polynomial in variable x_{n-1}. Since $\mathbb{K}$ is a finite field, one can use for example Berlekamp's algorithm to find these roots.

Next substitute the values of x_{n-1} obtained above and repeat the process.

A major question is what is the smallest D (denoted D_{min}) that allows for the XL-Algorithm to solve the system of equations.

There is no stopping in using this algorithm to solve systems of multivariate polynomials over a field of characteristic 0; we just don't use the results at the end of the algorithm that require the finite field assumption. This strategy that we are going to adopt is clearly explained in [5, Section 2].

We homogenize the equations with respect to a new variable x_n, to obtain $f_i(x_0, \ldots, x_n) \in R := \mathbb{K}[x_0, \ldots, x_n]$. Also let us assume that $\mathbb{K}$ is algebraically closed. Let $I \subset R$ be the ideal generated by $f_1, \ldots, f_m$.

Now we use the same principle of multiplying each equation $f_i(x_0, \ldots, x_n) = 0$ by all the monomials in variables $x_0, \ldots, x_n$ of degree exactly $D - \deg(f_i) = D - d_i$. We call the matrix of this system *the XL-matrix in degree D of the ideal I*.

The connection with inverse systems is done by direct inspection, observing the following:

Proposition 3.3. *The XL-matrix of degree D of the ideal I and the $D-$inverse system matrix $\mathcal{A}_{D,I}$ of I coincide.*

Remark 3.4. From [5], if $HF(R/I, D) \leq D$, then the first run of the XL-Algorithm is possible. Such a restriction on the Hilbert function forces in fact that $D \geq \deg(I)$. One way to show this comes from

$$D \geq HF(R/I, D) = HF(R/I, D-1) + HF(R/\langle I, \ell\rangle, D),$$

where ℓ is a nonzero divisor in R/I. If $D \leq reg(R/I)$, then $HF(R/\langle I, \ell\rangle, D) > 0$, forcing $D - 1 \geq HF(R/I, D-1)$. Inductively we get the contradiction $HF(R/I, 0) = 0$. So $D \geq reg(R/I) + 1$, and since $HF(R/I, reg(R/I) + 1) = \deg(I)$, we then must have

$$D \geq \deg(I).$$

The work of Diem and Mourrain-Pan in solving systems of equations is centered around the generic cases ([5, Definitions 3 and 4] and [17, Definition 4.2.4]), to obtain information on the complexity of the algorithms they analyze. Since our focus is not primarily computational, but rather methodological, from the Remark 3.4 above we pick $D = \deg(I)$, for any ideal I, and we find $X = Z(I)$ from $(I^{-1})_D$, using the XL-Algorithm via Proposition 3.3. In this way we basically replace the Gaussian elimination step in the XL-Algorithm with inverse systems.

Below is a simple example.

Example 3.5. Find $X = Z(I)$, where

$$I = \langle \underbrace{x_1^2 - x_0x_2}_{f_1}, \underbrace{x_0^2 - x_1x_2}_{f_2} \rangle.$$

Also assume that $\mathbb{K}$ is the field of complex numbers.

I is a complete intersection of two quadrics, so $D = \deg(I) = 4$.

The inverse system of degree 4 is

$$(I^{-1})_4 = \{ \sum_{j_0+j_1+j_2=4} b_{j_0,j_1,j_2} y_0^{j_0} y_1^{j_1} y_2^{j_2} = F \in S | f_1 \circ F = 0 \text{ and } f_2 \circ F = 0 \}.$$

We find basis for $(I^{-1})_4$ to be:

$$\begin{aligned} F_1 &= 2y_0^4 + 24y_0^2y_1y_2 + 8y_0y_1^3 + 8y_0y_2^3 + 12y_1^2y_2^2 \\ F_2 &= 4y_0^3y_1 + 6y_0^2y_2^2 + 12y_0y_1^2y_2 + y_1^4 + 4y_1y_2^3 \\ F_3 &= 2y_0^3y_2 + 3y_0^2y_1^2 + 6y_0y_1y_2^2 + 2y_1^3y_2 \\ F_4 &= y_2^4. \end{aligned}$$

One needs to find a polynomial of degree 4 in I in variables x_1 and x_2. This means we need

$$f = a_1x_1^4 + a_2x_1^3x_2 + a_3x_1^2x_2^2 + a_4x_1x_2^3 + a_5x_2^4 \text{ with } f \circ F_i = 0, i = 1, 2, 3, 4.$$

In the end we get

$$f = \alpha(x_1^4 - x_1x_2^3), \alpha \in \mathbb{K} - \{0\},$$

which has four distinct solutions, that give the last two homogeneous coordinates of the points in $V(I)$.

One needs to mention that without using any algorithm, this polynomial can be determined immediately as a result of trying to eliminate from f_1 and f_2 all monomials that contain x_0. Observe that $(x_1^2 - f_1)^2 = x_0^2x_2^2 = x_2^2(f_2 + x_1x_2)$ leading to

$$x_1^4 - x_1x_2^3 = -f_1^2 + 2x_1^2f_1 + x_2^2f_2.$$

REFERENCES

[1] J. Brachat, Schémas de Hilbert, Décomposition de tenseurs, Thèse, Univ. de Nice-Sophia-Antipolis, Juillet, 2011.

[2] J. Brachat, P. Comon, B. Mourrain, E.P. Tsigaridas, Symmetric tensor decomposition, Linear Alg. Appl. 433 (2010), 1851–1872.

[3] Y.H. Cho, A. Iarrobino, Inverse Systems of Zero-dimensional Schemes in $\mathbb{P}^n$, J. Algebra 366 (2012), 42–77.

[4] N. Courtois, A. Klimov, J. Patarin, A. Shamir, Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations, in B. Preneel (ed.): Advances in Cryptography - EUROCRYPT 2000, LNCS vol. 1807, pp. 392–407, Springer-Verlag, Berlin, 2000.
[5] C. Diem, The XL-Algorithm and a Conjecture from Commutative Algebra, in Advances in Cryptology - ASIACRYPT 2004, Proceedings of 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, LNCS vol. 3329, pp. 323–337, Springer 2004.
[6] E. Davis, A.V. Geramita, F. Orecchia, Gorenstein algebras and the Cayley-Bacharach theorem, Proc. Amer. Math. Soc. 93 (1985), 593-597.
[7] J. Emsalem, A. Iarrobino, Inverse system of a symbolic power I, J. Algebra 174 (1995), 1080–1090.
[8] A.V. Geramita, Inverse Systems of Fat Points: Waring's Problem, Secant Varieties of Veronese Varieties, and Parameter Spaces for Gorenstein Ideals, Queens Papers Pure Appl. Math. 102 (1996), 1–114.
[9] A.V. Geramita, H.K. Schenck, Fat points, inverse systems, and piecewise polynomial functions, J. Algebra 204 (1998), 116–128.
[10] B. Harbourne, A. Seceleanu, H.K. Schenck, Inverse systems, Gelfand-Tsetlin patterns and the weak Lefschetz property, J. London Math. Society 84 (2011), 712–730.
[11] A. Iarrobino, V. Kanev, Power Sums, Gorenstein Algebras, and Determinantal Loci, Lecture Notes in Mathematics 1721, Springer, Heidelberg, 1999.
[12] A. Kustin, B. Ulrich, If the socle fits, J. Algebra 147 (1992), 63–80.
[13] F.S. Macaulay, The algebraic theory of modular systems, Cambridge University, 1916.
[14] J.C. Migliore, R.M. Mir-Roig, U. Nagel, On the Weak Lefschetz Property for Powers of Linear Forms, arXiv: 1008.2149, Algebra Number Theory 2010, in press.
[15] J.C. Migliore, U. Nagel, Liaison and Related Topics, Rend. Sem. Mat. Univ. Pol. Torino 59 (2001), 59–126.
[16] J.C. Migliore, U. Nagel, A tour of the Weak and Strong Lefschetz Properties, arXiv: 1109.5718, 2011.
[17] B. Mourrain, V.Y. Pan, Multivariate Polynomials, Duality, and Structured Matrices, J. Complexity 16 (2000), 110–180.
[18] B. Reznick, Homogeneous Polynomial Solutions to Constant Coefficient PDE's, Adv. Math. 117 (1996), 179–192.
[19] H.K. Schenck, Computational Algebraic Geometry, London Mathematical Society Student Texts 58, Cambridge University Press, New York, 2003.
[20] P.F. Stiller, Vector Bundles on Complex Projective Spaces and Systems of Partial Differential Equations I, Trans. Amer. Math. Soc. 298 (1986), 537–548.